(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平7－170280

(43)公開日　平成７年(1995)７月４日

(51)Int.Cl.⁶	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　12/40				
9/00				
9/10				
		7341－5K	Ｈ０４Ｌ　11/ 00　　３２０	
			9/ 00　　Ｚ	

審査請求　未請求　請求項の数３　ＯＬ　（全　９　頁）　最終頁に続く

(21)出願番号　特願平5－314617

(22)出願日　平成５年(1993)12月15日

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号

(72)発明者　小林　秀樹
東京都大田区中馬込１丁目３番６号　株式会社リコー内

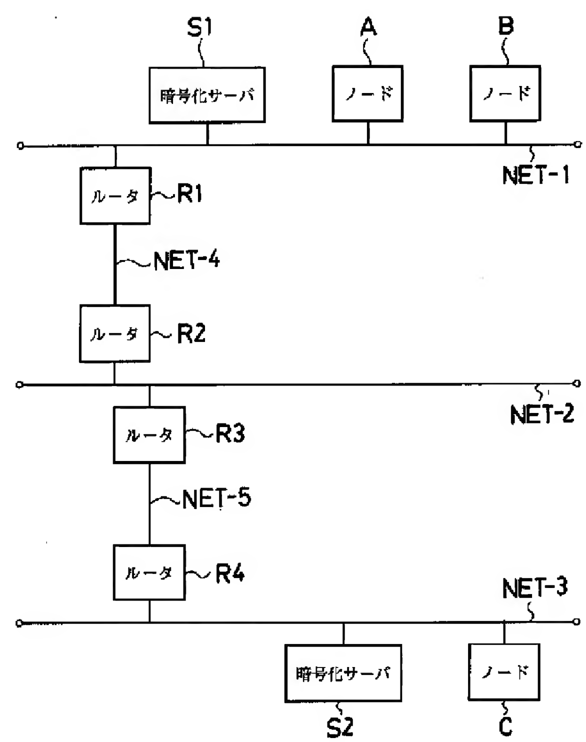
(74)代理人　弁理士　大澤　敬

(54)【発明の名称】　ローカルエリアネットワーク

(57)【要約】

【目的】　各端末装置でデータの暗号化と復号化を行なわなくても端末装置間でデータを暗号化して送受信できるようにする。

【構成】　ＩＰネットワークＮＥＴ－１の送信元の端末装置であるノードＡから送信される元データを暗号化サーバＳ１が暗号化データに変換してノードＡへ返送し、ノードＡはその暗号化されたデータをＩＰネットワークＮＥＴ－３の送信元の端末装置であるノードＣへ送る。一方、ＩＰネットワークＮＥＴ－３の受信先の端末装置であるノードＣから送信される暗号化データを暗号化サーバＳ２が解読して元データに復元してノードＣへ返送する。



【特許請求の範囲】

【請求項１】　複数の端末装置間でデータを送受信可能にネットワークで接続し、該ネットワークに、送信元の端末装置から送信される元データを暗号化データに変換して該送信元の端末装置へ返送し、受信先の端末装置から送信される暗号化データを解読して元データに復元して該受信先の端末装置へ返送する手段を有する暗号化サーバを設けたことを特徴とするローカルエリアネットワーク。

【請求項２】　複数の端末装置間でデータを送受信可能に接続したネットワークを複数接続し、該各ネットワークに、送信元の端末装置から送信される元データを暗号化データに変換して他のネットワークの受信先の端末装置へ送信し、他のネットワークから受信した暗号化データを解読して元データに復元して受信先の端末装置へ送信する手段を有する暗号化サーバを設けたことを特徴とするローカルエリアネットワーク。

【請求項３】　請求項１記載のローカルエリアネットワークにおいて、

前記各端末装置が、前記暗号化サーバに対してデータの暗号化又はその解読に必要な暗号化キーを送信する手段を有し、前記暗号化サーバが、前記各端末装置から受信した暗号化キーに基づいてデータの暗号化又はその解読を行なう手段を有することを特徴とするローカルエリアネットワーク。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明は、複数の端末装置をネットワークを介して接続したローカルエリアネットワークに関する。

【０００２】

【従来の技術】従来、ＥｔｈｅｒｎｅｔやＩＥＥＥ８０２．３等の規格のローカルエリアネットワーク（以下「ＬＡＮ」と略称する）では、各端末装置（以下「ノード」と略称する）間で送受信するパケットの内容の秘密を守るため、送信側のノードで送信すべきパケットの内容を所定の暗号系によって暗号化して相手先のノードへ送信し、その相手先である受信側のノードではその受信した暗号化されたパケットを解読して元のデータ内容に復元していた。

【０００３】この暗号系は、誰が読んでも理解できる情報を予め決められた暗号化キー（単に「キー」とも称する）に基づいて意味の分からない暗号文に変換し、その暗号文を暗号化されたときに使用した同じ暗号化キーに基づいて解読して元の情報に復元（これを「復号化」と称する）する技術である。

【０００４】一般に、暗号系としては標準暗号に制定されているＤＥＳ暗号法，ＦＥＡＬ暗号法等の共通キー暗号系が知られており、その共通キー暗号系は、送受信者間で等しい暗号化キーと復号化キーを共有し、その共通のキーでデータの暗号化と復号（復元）化を行なう方法である。

【０００５】

【発明が解決しようとする課題】しかしながら、上述した従来のＬＡＮでは、通信の秘密を守るためのパケットの暗号化が標準化（規格化）されていないため、送信側のノードでパケットの内容を暗号化して送信し、受信側のノードでその受信したパケットの暗号化されたデータ内容を解読して元のデータに復元しなければならなかった。

【０００６】したがって、各ノードの処理負担がかかってしまううえに、暗号化キーの変更や暗号系（暗号化方式）の変更時に、ＬＡＮ上の全てのノードの設定変更を行なわなければならなくなって大変不便であるという問題があった。

【０００７】また、ローカルなネットワーク環境ではネットワークが管理状態に置かれていおり、または管理し易いので、ネットワークの信頼性は高いが、外部のネットワークを介して複数のネットワーク間の端末装置間で通信を行なえるようにした場合、データがどのようなネットワークの経路を通って送受信されて相手に到達するのか分からないので、途中で外部のものにデータ内容を覗かれてしまう危険があるという問題も有った。

【０００８】この発明は上記の点に鑑みてなされたものであり、各端末装置でデータの暗号化と復号化を行なわなくても端末装置間でデータを暗号化して送受信できるようにすることを目的とする。

【０００９】

【課題を解決するための手段】この発明は上記の目的を達成するため、複数の端末装置間でデータを送受信可能にネットワークで接続し、そのネットワークに、送信元の端末装置から送信される元データを暗号化データに変換してその送信元の端末装置へ返送し、受信先の端末装置から送信される暗号化データを解読して元データに復元してその受信先の端末装置へ返送する手段を有する暗号化サーバを設けたローカルエリアネットワークを提供する。

【００１０】また、複数の端末装置間でデータを送受信可能に接続したネットワークを複数接続し、その各ネットワークに、送信元の端末装置から送信される元データを暗号化データに変換して他のネットワークの受信先の端末装置へ送信し、他のネットワークから受信した暗号化データを解読して元データに復元して受信先の端末装置へ送信する手段を有する暗号化サーバを設けたローカルエリアネットワークも提供する。

【００１１】さらに、上記のようなローカルエリアネットワークにおいて、上記各端末装置が、上記暗号化サーバに対してデータの暗号化又はその解読に必要な暗号化キーを送信する手段を有し、上記暗号化サーバが、上記各端末装置から受信した暗号化キーに基づいてデータの

暗号化又はその解読を行なう手段を有するようにするとよい。

【０　０　１　２】

【作用】この発明によるローカルエリアネットワークは、ネットワークに設けた暗号化サーバが、送信元の端末装置から送信される元データを暗号化データに変換してその送信元の端末装置へ返送し、受信先の端末装置から送信される暗号化データを解読して元データに復元してその受信先の端末装置へ返送するので、各端末装置でデータの暗号化と復号化を行なわなくても端末装置間でデータを暗号化して送受信できる。

【０　０　１　３】また、それぞれ接続された複数のネットワークに設けた暗号化サーバが、送信元の端末装置から送信される元データを暗号化データに変換して他のネットワークの受信先の端末装置へ送信し、他のネットワークから受信した暗号化データを解読して元データに復元して受信先の端末装置へ送信するので、各端末装置でデータの暗号化と復号化を行なわなくても異なるネットワーク間の端末装置間でデータを暗号化して送受信できる。

【０　０　１　４】さらに、各端末装置が、暗号化サーバに対してデータの暗号化又はその解読に必要な暗号化キーを送信し、暗号化サーバが、各端末装置から受信した暗号化キーに基づいてデータの暗号化又はその解読を行なうようにすれば、その暗号化キーに基づく暗号化方式によって暗号化及び復号化を行なえる。

【０　０　１　５】

【実施例】以下、この発明の実施例を図面に基づいて具体的に説明する。図１は、この発明の一実施例のローカルエリアネットワーク（ＬＡＮ）のシステム構成を示す図である。このローカルエリアネットワークではＴＣＰ／ＩＰプロトコルを用いている。このローカルエリアネットワークは、３つのＩＰネットワークＮＥＴ－１，ＮＥＴ－２，ＮＥＴ－３がある。

【０　０　１　６】ＩＰネットワークＮＥＴ－１には、ＣＰＵ，ＲＯＭ，及びＲＡＭからなるマイクロコンピュータを内蔵した端末装置（ノード）ＡとＢが接続されており、同じくマイクロコンピュータを備えた端末装置の一種であってノードＡとＢのデータを暗号化及びその解読（復元）をする暗号化サーバＳ１が接続されており、２ネットワーク間でパケットのルーティングを行なうルータ（「ゲートウェイ」とも称する）Ｒ１が接続されている。

【０　０　１　７】また、ＩＰネットワークＮＥＴ－２には、２ネットワーク間でパケットのルーティングを行なうルータＲ２とＲ３が接続されている。さらに、ＩＰネットワークＮＥＴ－３には、マイクロコンピュータを内蔵したノードＣが接続されており、同じくマイクロコンピュータを備えた端末装置の一種であってノードＣのデータを暗号化及びその解読（復元）をする暗号化サーバＳ２が接続されており、２ネットワーク間でパケットのルーティングを行なうルータＲ４が接続されている。

【０　０　１　８】そして、ルータＲ１とＲ２はネットワークＮＥＴ－４によって結ばれており、ルータＲ３とＲ４はネットワークＮＥＴ－５によって結ばれており、ＩＰネットワークＮＥＴ－１とＮＥＴ－３の各ノードＡ，Ｂ，Ｃ間でデータを送受信することができ、その際、暗号化サーバＳ１とＳ２によってデータを暗号化し、受信した暗号化データを復号化する（これを「暗号化通信」と称する）ことができる。

【０　０　１　９】上記暗号化サーバＳ１とＳ２は、送信元の端末装置から送信される元データを暗号化データに変換してその送信元の端末装置へ返送し、受信先の端末装置から送信される暗号化データを解読して元データに復元してその受信先の端末装置へ返送する手段を有しており、この場合、暗号化及びその解読のための暗号化キーは同じであって暗号化アルゴリズムが同じである。

【０　０　２　０】図２は、ＩＰネットワークＮＥＴ－１のノードＡからＩＰネットワークＮＥＴ－３のノードＣへ暗号化通信を行なうときのデータの流れを示すフローチャートである。ここでは、暗号化サーバＳ１とＳ２の暗号化キー（キーコード）は固定されている場合について説明する。

【０　０　２　１】まず、初期化時、ノードＡはローカルエリアネットワークの暗号化サーバＳ１のアドレスを登録し、ノードＣはローカルエリアネットワークの暗号化サーバＳ２のアドレスを登録する。

【０　０　２　２】ノードＡは、１パケットの送信要求が発生すると、暗号化サーバＳ１へ「暗号化要求フラグ」を立てて生データを送信する。暗号化サーバＳ１は、ノードＡから受信した生データを暗号化キーを用いて予め設定されている暗号化方式によって暗号化し、「暗号化済フラグ」を立ててノードＡへ返送する。

【０　０　２　３】そして、ノードＡは暗号化サーバＳ１から受信した暗号化データを暗号化データを示す情報を付加してＩＰネットワークＮＥＴ－３のノードＣへ送信（転送）する。その暗号化データであることを示す情報は、暗号化データのパケットのヘッダ部に格納すると良い。

【０　０　２　４】一方、ノードＣは、ノードＡから受信したパケットのヘッダ部を調べて、暗号化データであることを示す情報が格納されていれば、そのパケットが暗号化データであると判断し、その暗号化データに「解読要求フラグ」を立てて暗号化サーバＳ２へ転送する。暗号化サーバＳ２は、ノードＣから受信した暗号化データを暗号化キーを用いて解読して復元し、「解読済フラグ」をセットしてノードＣへ返送する。ノードＣは、暗号化サーバＳ２から復元されたデータを得る。

【０　０　２　５】このようにして、ネットワーク毎にデータの暗号化及びその解読を行なう暗号化サーバを設け、その暗号化サーバがネットワーク上の各端末装置に送受信されるデータの暗号化及びその解読を一括して処理する

ので、各端末装置がデータの暗号化及びその解読に係る処理を行なわずに済む。

【００２６】図４はパケットのＩＰヘッダのフォーマットを示す図、図５はそのＩＰヘッダの「（オプション）Ｏｐｔｉｏｎｓ」フィールドのフォーマットを示す図である。上記の暗号化要求フラグ，暗号化済フラグ，解読要求フラグ，及び解読済フラグはＩＰヘッダの「Ｏｐｔｉｏｎｓ」フィールドのオプションエリアに定義する。

【００２７】表１はオプション・データの一例を示す表であり、上記各フラグは、例えば、暗号化要求フラグ「０」，暗号化済フラグ「１」，解読要求フラグ「３」，解読済フラグ「４」である。

【００２８】

【表１】

Class	Number	長さ	機能
0	0	1	オプション・リストの終わり
0	1	1	NOP(オペレーション無し)
0	2	11	セキュリティと処理に対する制約
0	3	可変	Loose Source Routing
0	9	可変	Strict Source Routing
0	7	可変	ルート記録
0	8	4	ストリーム識別子
2	4	可変	時刻印
1	1	1	フラグ 0　暗号化要求 1　解読要求 2　暗号化済 3　解読済

【００２９】次に、ＩＰネットワークＮＥＴ－１のノードＡからＩＰネットワークＮＥＴ－３のノードＣへ暗号化通信を行なうとき、データの暗号化及びその解読のための暗号化キーを暗号化サーバＳ１とＳ２へ送る場合の例について説明する。

【００３０】この場合、各ノードＡ，Ｃはデータの暗号化又は解読のための暗号化キーを暗号化サーバＳ１，Ｓ２へ送信する機能を有し、暗号化サーバＳ１，Ｓ２は複数の暗号化キーを用いた暗号化及びその解読方式を行なう機能をそなえており、ノードＡ，Ｃから送信される暗号化キーを用いてデータの暗号化及びその解読を行なう機能を果たす。

【００３１】まず、ノードＡはノードＣとの間で暗号化データをやり取りするために必要な暗号化キーの共通化を図る初期化通信を行なう。この初期化通信によって、ノードＡとノードＣは同じ暗号化方式の暗号化キーを所持することになる。

【００３２】そして、ノードＡから暗号化サーバＳ１へ元データを送るとき、暗号化キーを貼付し、暗号化サーバＳ１はその暗号化キーを使用して元データを暗号化する。また、暗号化データの解読時には、ノードＣは暗号化サーバＳ２へ解読を依頼するときその暗号化キーを添付し、暗号化サーバＳ２はその暗号化キーを使用して暗号化データを復元する。暗号化キーは、例えば、図４及び図５に示したＩＰヘッダの「オプション・データ」に定義する。

【００３３】ノードＡは、１パケットの送信要求が発生すると、暗号化サーバＳ１へ「暗号化要求フラグ」を立てて暗号化キーと共に生データを送信する。暗号化サーバＳ１は、ノードＡから受信した生データをその暗号化キーを用いた暗号化方式によって暗号化し、「暗号化済フラグ」を立ててノードＡへ返送する。そして、ノードＡは暗号化サーバＳ１から受信した暗号化データをＩＰネットワークＮＥＴ－３のノードＣへ送信（転送）する。

【００３４】一方、ノードＣはノードＡから暗号化データを受信すると、その暗号化データを「解読要求フラグ」を立てて暗号化キーと共に暗号化サーバＳ２へ転送する。暗号化サーバＳ２は、ノードＣから受信した暗号化データをその暗号化キーを用いた解読方式によって復元し、「解読済フラグ」をセットしてノードＣへ返送する。ノードＣは、暗号化サーバＳ２から復元されたデータを得る。したがって、このＬＡＮではキーコードを可変にすることができる。

【００３５】次に、ＩＰネットワークＮＥＴ－１のノードＡからノードＢへ暗号化通信を行なうとき、データの暗号化及びその解読のための暗号化キーを暗号化サーバＳ１へ送る例について説明する。

【００３６】ノードＡは、１パケットの送信要求が発生すると、暗号化サーバＳ１へ「暗号化要求フラグ」を立てて暗号化キーと共に生データを送信する。暗号化サーバＳ１は、ノードＡから受信した生データをその暗号化キーを用いた暗号化方式によって暗号化し、「暗号化済フラグ」を立ててノードＡへ返送する。そして、ノードＡは暗号化サーバＳ１から受信した暗号化データをノードＢへ送信（転送）する。

【００３７】一方、ノードＢはノードＡから暗号化データを受信すると、その暗号化データを「解読要求フラグ」を立てて暗号化キーと共に暗号化サーバＳ１へ転送する。暗号化サーバＳ１は、ノードＢから受信した暗号化データをその暗号化キーを用いた解読方式によって復元し、「解読済フラグ」をセットしてノードＢへ返送する。ノードＢは、暗号化サーバＳ１から復元されたデータを得る。

【００３８】このようにして、各端末装置が暗号化サーバにデータの暗号化及びその解読を依頼するとき、データと共にその暗号化及び解読に必要な暗号化キーを送り、暗号化サーバは、その暗号化キーに基づいた暗号化方式でデータの暗号化及びその解読を行なうので、各端末装置では多様な暗号化方式によるデータ送受信を容易に利用することができる。また、各ノードが自由に暗号化キーを設定して、データの暗号化方式を選択できるので、さらにデータ通信の機密性を高めることができる。

【００３９】次に、暗号化サーバにネットワークルーティング機能を設けたときの暗号化通信の例について説明する。この場合のネットワーク構成は図１に示したローカルエリアネットワークと同じであるが、各ノードＡ，Ｂ，Ｃと暗号化サーバＳ１，Ｓ２の機能が若干異なる。

【００４０】この例の暗号化サーバＳ１とＳ２は、送信元の端末装置から送信される元データを暗号化データに変換して他のネットワークの受信先の端末装置へ送信し、他のネットワークから受信した暗号化データを解読して元データに復元して受信先の端末装置へ送信する手段を備えている。

【００４１】したがって、上述の暗号化サーバＳ１，Ｓ２にネットワーク層のネットワークルーティング機能（ルータ）を設け、暗号化サーバＳ１はノードＡの代理ＡＲＰをするノードとしての働きをする。

【００４２】ＩＰネットワークでは、１ネットワーク上に複数のルータが存在させることができ、実際の通信ではアドレス・リゾリューション・プロトコル（ＡＲＰ）によってＩＰアドレスから物理アドレス（ＭＡＣアドレス）を求め、その物理アドレスで通信相手を指定して通信を行なう（データリンク層）。普通は、物理アドレスは通信相手が返してきたものを使用するが、別のノードがそれを返すこともできる。これを代理ＡＲＰと称する。

【００４３】そして、各ネットワークにネットワークルータ機能と受信ノードの代わりにパケットを受け取る代理応答機能を備えた暗号化サーバを設ける。送信側のネットワークの送信ノードは、この暗号化サーバへ通信の秘密を守りたいデータのみを送り、暗号化サーバはそのデータを暗号化データに変換してネットワークルータ機能によってそのデータの受信先のネットワークへ送信する。

【００４４】一方、受信側のネットワークの暗号化サーバは、受信ノードの代わりにパケットを受け取る代理応答機能によって送信側ネットワークから送信されたパケット（暗号化データ）を受信し、それを解読して復元し、その復元されたデータを受信ノードへ送信する。

【００４５】図３は、ＩＰネットワークＮＥＴ－１のノードＡからＩＰネットワークＮＥＴ－３のノードＣへ暗号化通信を行なうときのデータの流れを示すフローチャートである。ここでは、暗号化サーバＳ１とＳ２の暗号化キー（キーコード）は固定されている場合について説明する。

【００４６】ノードＡは、初期化時、ローカルエリアネットワークの暗号化サーバＳ１のアドレスを登録し、その暗号化サーバＳ１を代理送受信するデフォルトルータとする。また、ノードＣは、初期化時、ローカルエリアネットワークの暗号化サーバＳ２のアドレスを登録し、その暗号化サーバＳ２を代理送受信するデフォルトルータとする。

【００４７】したがって、暗号化サーバＳ１はノードＡの代理ＡＲＰとしてノードＡへのデータを横取りし、同様に、暗号化サーバＳ２はノードＣの代理ＡＲＰをするノードとして働き、ノードＣへのデータを横取りする。

【００４８】ノードＡからノードＣへのデータ送信時、ノードＡは暗号化サーバＳ１に生データを送信する。暗号化サーバＳ１はその生データを暗号化後「暗号化済フラグ」を立ててルータＲ１へ転送する。その暗号化データは、ルータＲ１，Ｒ２，Ｒ３，Ｒ４の順番に転送されてノードＣの代理ノードとしての暗号化サーバＳ２に転送される。

【００４９】暗号化サーバＳ２はその暗号化データを受信して解読後、最後にノードＣへ転送する。ノードＣは暗号化サーバＳ２からノードＡによって送信された暗号化データを復元されたデータで受け取る。

【００５０】上記の第２実施例の暗号化サーバＳ１のルーティング機能は、受けたパケットを全てルータＲ１に渡すだけの機能が有れば十分であり、暗号化サーバＳ２のルーティング機能も、受けたパケットを全てルータＲ２に渡すだけの機能が有れば十分である。

【００５１】このようにして、複数のネットワークにまたがるパケット通信の場合、すなわち外部のネットワークの受信先ノードへデータを出す場合、送信側のノードが暗号化サーバへ受信先ノードを指定して通信の秘密を守りたいデータを送信すれば、その暗号化サーバが直接受信先ノードのネットワークへ通信する。

【００５２】したがって、送信側ノードは暗号化サーバにデータの暗号化を依頼して、暗号化されたデータを自ら受信先ノードへ送信することなく、暗号化サーバとのデータのやり取りを簡略化することができ、つまり、ノードと暗号化サーバとの１往復分のデータのやり取りの時間とトラフィックを節約でき、送信側ノードの処理負担を軽減し、データ通信の高速性及び効率性を図ること

ができる。

【００５３】また、受信側ノードは、自己のネットワークに接続されている暗号化サーバによって送信側ノードから送信された暗号化データを復元された状態で受け取ることができるので、同様にノードと暗号化サーバとの１往復分のデータのやり取りの時間とトラフィックを節約でき、受信側ノードの処理負担を軽減し、データ通信の高速性及び効率性を図ることができる。

【００５４】

【発明の効果】以上説明してきたように、この発明によるローカルエリアネットワークによれば、ネットワークの各端末装置毎にデータの暗号化と復号化を行なわず、暗号化サーバによって集中して行なうので、各端末装置の処理負荷を軽減させることができ、ネットワークにおける暗号化キーの変更や暗号化方式の変更時にはその暗号化サーバの設定を変更するだけでよいので、それぞれの端末装置の設定を変更する煩雑な作業を行なわずに済み、ネットワークの管理を容易に行なえる。

【００５５】また、外部のネットワークを介して複数のネットワーク間の端末装置間で通信を行なえるようにしたとき、データがどのようなネットワークの経路を通って送受信されても途中で外部のものにデータ内容を覗かれてしまう危険がない。

【００５６】さらに、ネットワークの各端末装置が、暗号化サーバに対してデータの暗号化又はその解読に必要な暗号化キーを送信し、暗号化サーバが、各端末装置から受信した暗号化キーに基づいてデータの暗号化又はその解読を行なうようにすれば、多様な暗号化方式を容易に利用することができる。

【図面の簡単な説明】

【図１】この発明の一実施例のローカルエリアネットワーク（ＬＡＮ）のシステム構成を示す図である。

【図２】図１のノードＡからノードＣへ暗号化通信を行なうときのデータの流れを示すフローチャートである。

【図３】図１の暗号化サーバＳ１とＳ２のルーティング機能を用いてノードＡからノードＣへ暗号化通信を行なうときのデータの流れを示すフローチャートである。

【図４】各ノード間で送受信されるパケットのＩＰヘッダのフォーマットを示す図である。

【図５】図４のＩＰヘッダの「オプション（Ｏｐｔｉｏｎｓ）」フィールドのフォーマットを示す図である。

【符号の説明】

Ａ～Ｃ：端末装置（ノード）

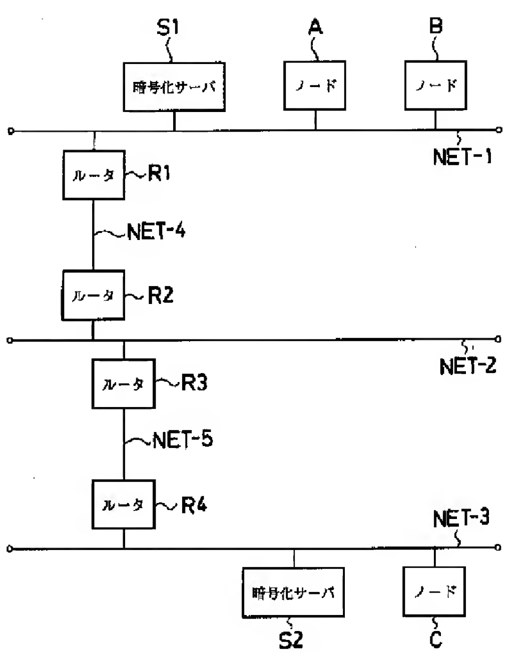
Ｓ１，Ｓ２：暗号化サーバ

Ｒ１～Ｒ４：ルータ

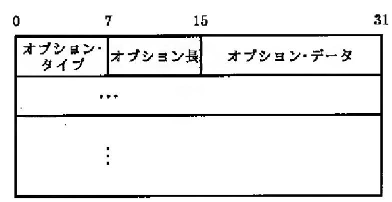
ＮＥＴ－１～ＮＥＴ－３：ＩＰネットワーク

ＮＥＴ－４，ＮＥＴ－５：ネットワーク

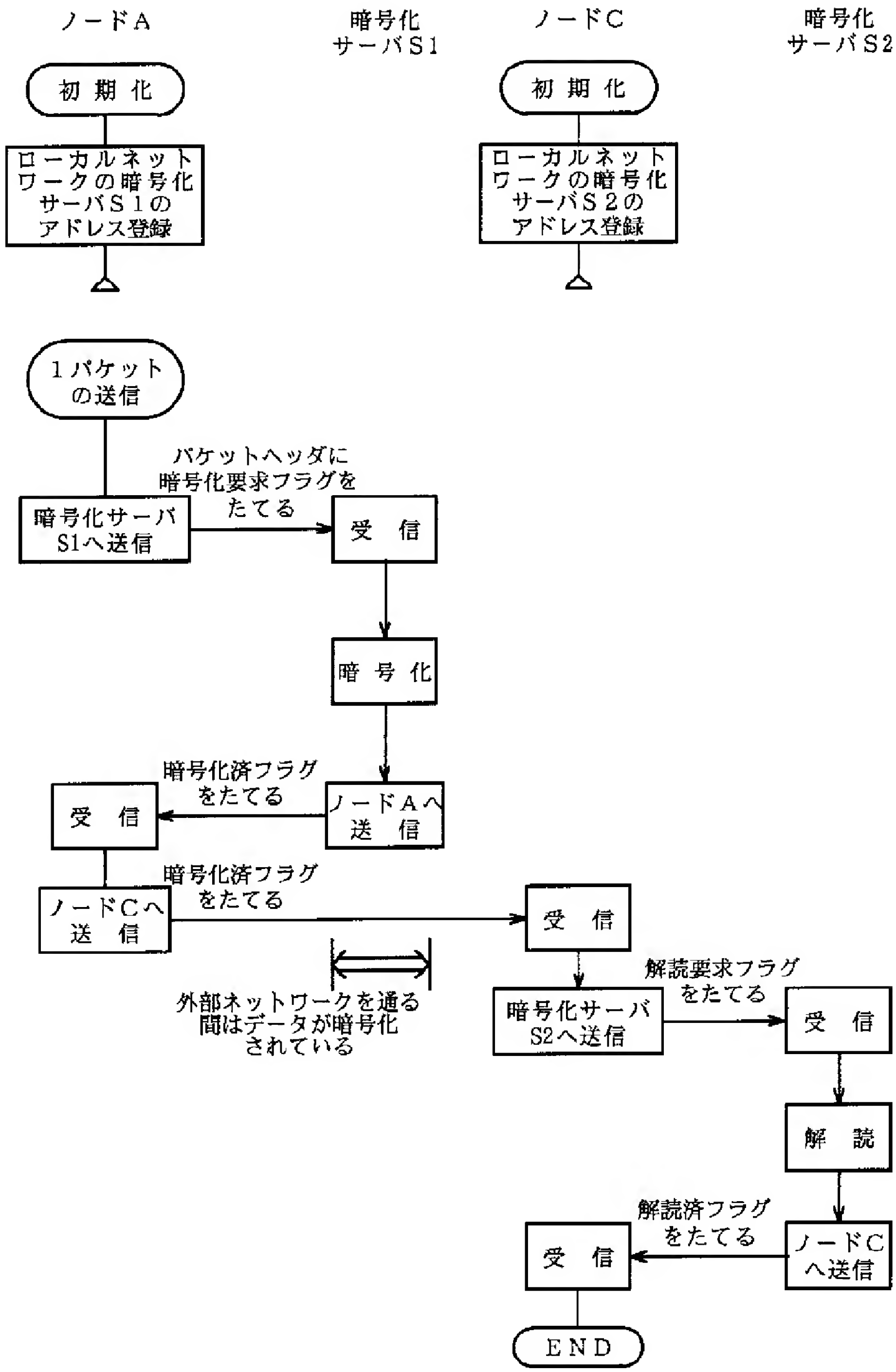
【図１】



【図５】

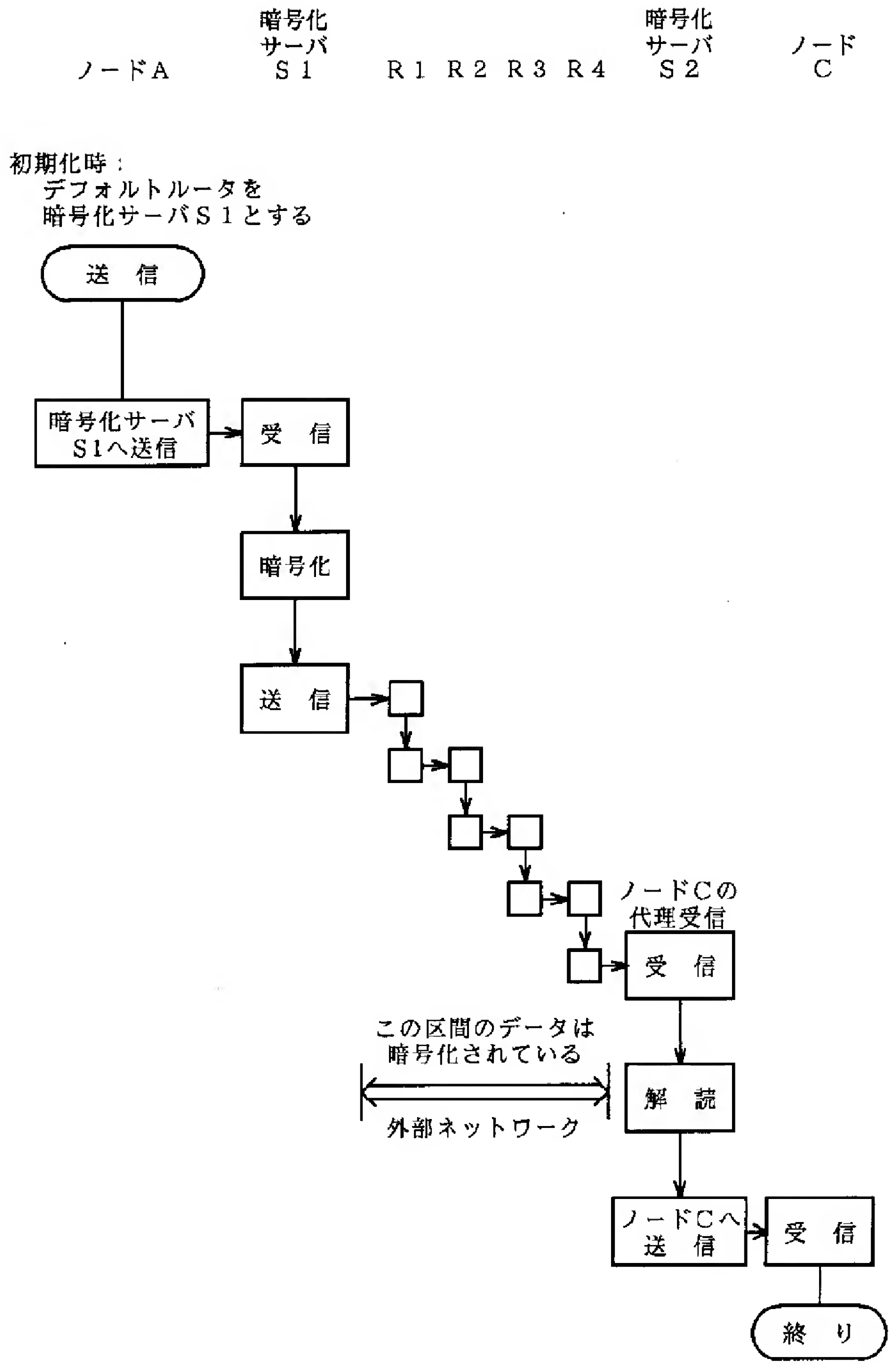


【図２】



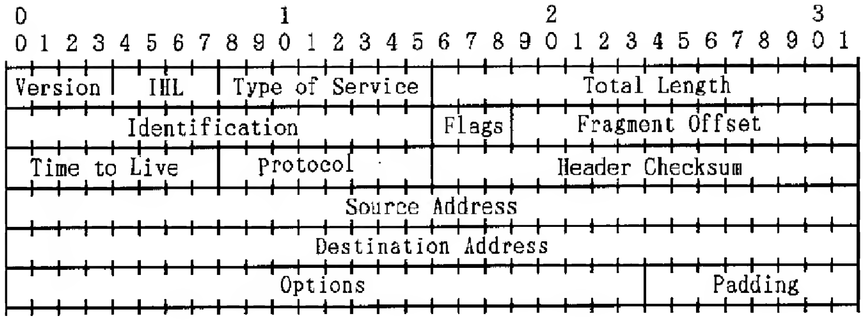
ノードＡ
暗号化
サーバＳ１
ノードＣ
暗号化
サーバＳ２
初 期 化
ローカルネットワークの暗号化サーバＳ１のアドレス登録
初 期 化
ローカルネットワークの暗号化サーバＳ２のアドレス登録
１パケットの送信
暗号化サーバS1へ送信
パケットヘッダに暗号化要求フラグをたてる
受 信
暗 号 化
ノードＡへ送 信
暗号化済フラグをたてる
受 信
ノードＣへ送 信
暗号化済フラグをたてる
受 信
外部ネットワークを通る間はデータが暗号化されている
暗号化サーバS2へ送信
解読要求フラグをたてる
受 信
解 読
ノードＣへ送信
解読済フラグをたてる
受 信
ＥＮＤ

【図３】



暗号化
サーバ
Ｓ１
暗号化
サーバ
Ｓ２
ノードＡ
Ｒ１　Ｒ２　Ｒ３　Ｒ４
ノード
Ｃ
初期化時：
デフォルトルータを
暗号化サーバＳ１とする
送　信
暗号化サーバ
Ｓ1へ送信
受　信
暗号化
送　信
ノードＣの
代理受信
受　信
この区間のデータは
暗号化されている
外部ネットワーク
解　読
ノードＣへ
送　信
受　信
終　り

【図４】



フロントページの続き

(51)Int.Cl.^{6}	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/12				

(54) [TITLE OF THE INVENTION] LOCAL AREA NETWORK

(57) [ABSTRACT]

[OBJECT] To enable data to be encrypted and transmitted/received between terminal devices without encrypting and decoding the data between the respective terminal devices.

[CONSTITUTION] An encryption server S1 converts original data transmitted from a node A as a terminal device of a transmitting source of an IP network NET-1 into encrypted data so as to return to the node A, and the node A transmits the encrypted data to a node C as a terminal device of a transmitting source of an IP network NET-3. On the other hand, an encryption server S2 decrypts and restores the encrypted data transmitted from the node C as the terminal device of a receiving destination of the IP network NET-3 into original data so as to return it to the node C.

[CLAIMS]

[Claim 1] A local area network where a plurality of terminal devices are connected by a network so that data can be transmitted/received between the terminal devices, the network comprising an encryption server having a unit for converting original data transmitted from the terminal device of a transmitting source into encrypted data so as to return it to the terminal device as the transmitting source, decrypting the encrypted data transmitted from the terminal device of a receiving destination and restoring it into the original data so as to return the original data to the terminal device of the receiving source.

[Claim 2] A local area network where a plurality of networks is connected so that data can be transmitted/received between a plurality of terminal devices, each of the networks comprising an encryption server having a unit for converting original data transmitted from a terminal device of a transmitting source into encrypted data so as to transmit the encrypted data to a terminal device of a receiving destination of different network, decrypting the encrypted data received from different network and restoring it into the original data so as to transmit the original data to the terminal device of the receiving destination.

[Claim 3] The local area network according to claim 1, wherein

each of the terminal devices has a unit for transmitting an encryption key necessary for encrypting or decrypting data to the encryption server,

the encryption server has a unit for encrypting or decrypting the data based on the encryption key received from each of the terminal devices.

[Detailed Description of the Invention]

[0001]

[Field of Industrial Application] The present invention relates to a local area

network for connecting a plurality of terminal devices via the network.

[0002]

[Prior Art] Conventionally, in a local area network (hereinafter, " LAN") complying with standards of Ethernet or IEEE802.3, in order to keep secret of the contents of packets transmitted/received between respective terminal devices (hereinafter, "nodes"), the contents of the packets to be transmitted from on a node on a transmitting side are encrypted by a predetermined encryption system so as to be transmitted to a node of a destination node, and the received and encrypted packets are decrypted and restored into original data contents on the node on receiving side of the destination.

[0003] The encryption system is a technique that converts information understandable by anybody into meaningless code texts based on a predetermined encryption key (simply "key"), and decrypts the code texts using the same encryption key used in the encryption so as to restore them into the original information (referred to as "decoding").

[0004] In general, a common key encryption system such as a DES encryption method and an FEAL encryption method complying with standard encryption are known as the encryption system. In the common key encryption system, identical encryption key and decoding key are shared between transmitters and receivers, and data are encrypted and decoded (restored) by using the common key.

[0005]

[Problem to be Solved by the Invention] However, since the encryption of packets for keeping communication secrets is not standardized in the above conventional LAN, the contents of the packets should be encrypted at a node on a transmitting side so as to be transmitted, and the encrypted data contents of the received packets should be decrypted so as to be restored into

the original data at a node on a receiving sides.

[0006] Therefore, a processing load is put on the respective nodes, and further when the encryption key and the encryption system (decryption method) are changed, the settings of all the nodes on LAN should be changed. This is very inconvenient.

[0007] Further, in a local network environment, since a network is in a managed state or is easily managed, reliability of the network is high. However, communication is enabled between a plurality of terminal devices in a plurality of networks via an external network, routes of networks through which data are transmitted/received and reach a destination cannot be obtained. For this reason, there arises a problem that the data contents may be intercepted by outsiders on such routes.

[0008] The present invention is devised in view of the above point, and its object is to enable data to be encrypted and transmitted/received between terminal devices without encrypting and decoding in the respective terminal devices.

[0009]

[Means for Solving the Problem] In order to achieve the above object, the present invention provides a local area network where a plurality of terminal devices is connected by a network so that data can be transmitted/received between the terminal devices, the network comprising an encryption server having a unit for converting original data transmitted from the terminal device of a transmitting source into encrypted data so as to return it to the terminal device as the transmitting source, decrypting the encrypted data transmitted from the terminal device of a receiving destination and restoring it into the original data so as to return the original data to the terminal device of the receiving source.

[0010] Further, the invention provides a local area network where a plurality of networks is connected so that data can be transmitted/received between a plurality of terminal devices, each of the networks comprising an encryption server having a unit for converting original data transmitted from a terminal device of a transmitting source into encrypted data so as to transmit the encrypted data to a terminal device of a receiving destination of different network, decrypting the encrypted data received from different network and restoring it into the original data so as to transmit the original data to the terminal device of the receiving destination.

[0011] Further, in the above local area network, each of the terminal devices has a unit for transmitting an encryption key necessary for encrypting or decrypting data to the encryption server, and the encryption server has a unit for encrypting or decrypting the data based on the encryption key received from each of the terminal devices.

[0012]

[Function] In the local area network of the present invention, the encryption server provided to the network converts original data transmitted from the terminal device of the transmitting source into encrypted data and returns it to the terminal device of the transmitting source, decrypts the encrypted data transmitted from the terminal device of the receiving destination so as to restore it into the original data, and returns the original data to the terminal device of the receiving destination. For this reason, the data can be encrypted and transmitted/received between the terminal devices without encrypting and decrypting the data in the respective terminal devices.

[0013] Further, each of the encryption servers provided to a plurality of connected networks convert original data transmitted from the terminal device of the transmitting source into encrypted data so as to transmit it to a

terminal device of the receiving destination in different network, and decrypts the encrypted data received from the different network so as to restore it into the original data, and transmits the original data to the terminal device of the receiving destination. For this reason, the data can be encrypted and transmitted/received between terminal devices in the respective networks without encrypting and decoding the data in the respective terminal devices.

[0014] Further, each of the terminal devices transmits an encryption key necessary for encrypting and decrypting data to the encryption server, the encryption server encrypts or decrypts the data based on the encryption key received from each of the terminal devices. As a result, the encryption and decoding can be performed according to the encryption method based on the encryption key.

[0015]

[Embodiments] Embodiments of the present invention are described concretely below with reference to drawings. Fig. 1 is a diagram illustrating a system structure of a local area network (LAN) according to one embodiment of the present invention. This local area network uses a TCP/IP protocol. This local area network includes three IP networks NET-1, NET-2 and NET-3.

[0016] The IP network NET-1 is connected to terminal devices (nodes) A and B containing a microcomputer composed of CPU, ROM and RAM, and is connected to an encryption server S1 that is one kind of a terminal device having a microcomputer and encrypts and decrypts (restores) data of the nodes A and B, and is connected to a router (referred to as “gateway”) R1 for routing a packet between two networks.

[0017] Further, the IP network NET-2 is connected to routers R2 and R3 for routing a packet between two networks. Further, the IP network NET-3 is

connected to a node C containing a microcomputer, and is connected to an encryption server S2 that is one kind of a terminal device containing a microcomputer and encrypts and decrypts (restores) data of the node C. The IP network NET-3 is connected to a router R4 for routing a packet between two networks.

[0018] The routers R1 and R2 are connected by a network NET-4, and the routers R3 and R4 are connected by a network NET-5, so that data can be transmitted/received between the nodes A, B and C of the IP networks NET-1 and NET-3. At this time, the encryption servers S1 and S2 can encrypt the data and can decode the received encrypted data (referred to as "encrypted communication").

[0019] The encryption servers S1 and S2 have a unit for converting original data transmitted from a terminal device of a transmitting source into encrypted data so as to return the encrypted data to the terminal device of the transmitting source, and decrypting the encrypted data transmitted from a terminal device of a receiving destination and restoring it into the original data so as to return the original data to the terminal device of the receiving destination. In this case, the same encryption key and the same encryption algorithm are used for the encryption and the decryption.

[0020] Fig. 2 is a flowchart illustrating a flow of data when encrypted communication is held from the node A of the IP network NET-1 to the node C of the IP network NET-3. The case where an encryption key (key code) of the encryption servers S1 and S2 is fixed is described.

[0021] At first, at the time of initialization, the node A registers an address of the encryption server S1 in the local area network, and the node C registers an address of the encryption server S2 in the local area network.

[0022] When transmission for one packet is requested, the node A sets an

"encryption request flag" for the encryption server S1, so as to transmit raw data. The encryption server S1 encrypts the raw data received from the node A using an encryption key according to a preset encryption method, and sets an "encrypted flag" so as to return the data to the node A.

[0023] The node A adds information representing the encrypted data to the encrypted data received from the encryption server S1, and transmits (transfers) the encrypted data to the node C of the IP network NET-3. The information representing the encrypted data may be stored in a header section of the packet.

[0024] On the other hand, the node C checks the header section of the packet received from the node A, and when the information representing the encrypted data is stored, it determines that the packet is the encrypted data. The node C sets a "decryption request flag" for the encrypted data, and transfers the encrypted data to the encryption server S2. The encryption server S2 decrypts and restores the encrypted data received from the node C using the encryption key, and sets a "decrypted flag" so as to return the restored data to the node C. The node C acquires the restored data from the encryption server S2.

[0025] In such a manner, the encryption servers for encrypting and decrypting data are provided to respective networks, and the encryption servers collectively encrypt and decrypt data transmitted/received to/from the respective terminal devices on the networks. For this reason, each of the respective terminal devices does not have to encrypt and decrypt the data.

[0026] Fig. 4 is a diagram illustrating a format of the IP header of the packet, and Fig. 5 is a diagram illustrating a format of an "Options" field of the IP header. The encryption request flag, the encrypted flag, the decryption request flag and the decrypted flag are defined on an option area of the

"Options" field of the IP header.

[0027] Table 1 is a table illustrating one example of option data, and respective flags are, for example, the encryption request flag "0", the encrypted flag "1", the decryption request flag "3" and the decrypted flag "4".

[0028]

[Table 1]

Class	Number	Length	Function
0	0	1	End of Option List
0	1	1	NOP (No Operation)
0	2	11	Restriction on Security and Process
0	3	Variable	Loose Source Routing
0	9	Variable	String Source Routing
0	7	Variable	Record Route
0	8	4	Stream Identifier
2	4	Variable	Time Stamp
1	1	1	Flag 0: Encryption Request 1: Decryption Request 2: Encrypted 3: Decrypted

[0029] An example where when the encrypted communication is held from the node A of the IP network NET-1 to the node C of the IP network NET-3, an encryption key for encrypting and decrypting data is transmitted to the encryption servers S1 and S2 is described below.

[0030] In this case, the nodes A and C have a function for transmitting the encryption key for encrypting or decrypting data to the encryption servers S1

and S2. The encryption servers S1 and S2 have a function for performing the encryption and decryption methods using a plurality of encryption keys, and they encrypt and decrypt data using the encryption keys transmitted from the nodes A and C.

[0031] At first, the node A holds initialization communication that standardizes an encryption key necessary for exchanging encrypted data with the node C. This initialization communication provides the encryption key of the same encryption method to the nodes A and C.

[0032] When original data is transmitted from the node A to the encryption server S1, the encryption key is attached, and the encryption server S1 encrypts the original data using the encryption key. Further, at the time of decrypting the encrypted data, the node C attaches the encryption key when requesting the encryption server S2 to decrypt the encrypted data, and the encryption server S2 restores the encrypted data using the encryption key. The encryption key is defined in “option data” of the IP header shown in Figs. 4 and 5, for example.

[0033] When transmission request of one packet is generated, the node A sets the "encryption request flag" for the encryption server S1, and transmits raw data together with the encryption key. The encryption server S1 encrypts the raw data received from the node A according the encryption method using the encryption key, sets the "encrypted flag" and returns the data to the node A. The node A transmits (transfers) the encrypted data received from the encryption server S1 to the node C of the IP network NET-3.

[0034] On the other hand, when the node C receives the encrypted data from the node A, it sets the "decryption request flag" and transmits the encrypted data as well as the encryption key to the encryption server S2. The encryption server S2 restores the encrypted data received from the node C

according to the decryption method using the encryption key, and sets the "decrypted flag" so as to return the restored data to the node C. The node C obtains the restored data from the encryption server S2. Therefore, in this LAN, a key code is variable.

[0035] An example, that when the encrypted communication is held from node A of the IP network NET-1 to the node B, the encryption key for encrypting and decrypting data is transmitted to the encryption server S1, is described below.

[0036] When transmission request for one packet is generated, the node A sets the "encryption request flag" for the encryption server S1, and transmits raw data as well as an encryption key. The encryption server S1 encrypts the raw data received from the node A according to the encryption method using the encryption key, and sets the "encrypted flag" so as to return the data to the node A. The node A transmits (transfers) the encrypted data received from the encryption server S1 to the node B.

[0037] On the other hand, when the node B receives the encrypted data from the node A, it sets the "decryption request flag" and transfers the encrypted data as well as the encryption key to the encryption server S1. The encryption server S1 restores the encrypted data received from node B according to the decryption method using the encryption key, and sets the "decrypted flag" so as to return the restored data to the node B. The node B obtains the restored data from the encryption server S1.

[0038] In such a manner, when each terminal device requests the encryption server to encrypt and decrypt data, each of them transmits the encryption key necessary for the encryption and decryption together with the data, and the encryption server encrypts and decrypts the data according to the encryption method using the encryption key. For this reason, each of the terminal

devices can easily utilize the data transmission/reception according to various encryption methods. Further, since each node can freely set an encryption key and can select the encryption method for data, the secrecy of the data communication can be further heightened.

[0039] An example of the encrypted communication when a network routing function is provided to the encryption server is described below. The network structure in this case is the same as that of the local area network shown in Fig. 1, but the functions of the nodes A, B and C and the encryption servers S1 and S2 are slightly different.

[0040] The encryption servers S1 and S2 in this example has a unit for converting original data transmitted from the terminal device of the transmitting source into encrypted data so as to transmit the encrypted data to the terminal device of the receiving destination in different network, and decrypting the encrypted data received from another network so as to restore it into the original data and transmit it to the terminal device of the receiving destination.

[0041] Therefore, a network routing function (router) of a network layer is provided to the encryption servers S1 and S2, and the encryption server S1 functions as a node that is a substitute for the node A at which ARP is implemented.

[0042] In an IP network, a plurality of routers can be provided to one network, and in actual communication, a physical address (MAC address) is obtained from an IP address according to an address resolution protocol (ARP), and a communication destination is specified by the physical address so that communication is held (data link layer). Normally, the physical address that is returned from the communication destination is used, but a different node can return it. This is called as the substitute ARP.

[0043] Each network is provided with an encryption server having a network router function and a substitute response function for receiving a packet instead of a receiving node. A transmitting node of the network on a transmitting side sends only data whose communication secret is desired to be kept to the encryption server, and encryption server converts the data into the encrypted data so as to transmit the data to a network of a receiving destination of this data using the network router function.

[0044] On the other hand, the encryption server of the network on the receiving side receives the packet (encrypted data) transmitted from the network on the transmitting side using the substitute response function for receiving the packet instead of the receiving node, and restores the packet so as to transmit the restored data to the receiving node.

[0045] Fig. 3 is a flow chart illustrating a flow of data when the encrypted communication is held between the node A of the IP network NET-1 to the node C of the IP network NET-3. The case where an encryption key (key code) of the encryption servers S1 and S2 is fixed is described.

[0046] The node A registers an address of the encryption server S1 of the local area network at the time of initialization, and the encryption server S1 is used as a default router for carrying out substitute transmission/reception. Further, the node C registers an address of the encryption server S2 of the local area network at the time of initialization, and the encryption server S2 is used as a default router for carrying out substitute transmission/reception.

[0047] Therefore, the encryption server S1 intercepts the data to be transmitted to the node A as the substitute ARP of the node A, and similarly the encryption server S2 functions as the node for implementing the substitute ARP of the node C to intercept the data to be transmitted to the node C.

[0048] At the time of the data transmission from the node A to the node C, the node A transmits raw data to the encryption server S1. The encryption server S1 encrypts the raw data and sets the "encrypted flag" so as to transmit the encrypted data to the router R1. The encrypted data is transmitted to the routers R1, R2, R3 and R4 in this order, and then to the encryption server S2 substitute for the node C.

[0049] The encryption server S2 receives and decrypts the encrypted data, and finally transmits it to the node C. The node C receives the encrypted data transmitted by the node A from the encryption server S2 as the restored data.

[0050] As to the routing function of the encryption server S1 according to the second embodiment, it is only necessary to transmit all received packets to the router R1. As to the routing function of the encryption server S2, it is only necessary to transmit all received packets to the router R2.

[0051] In such a manner, in the case of the packet communication between a plurality of networks, namely, in the case where data is sent to a receiving destination node of an external network, when the node on the transmitting side specifies the receiving destination node and transmits data whose communication secret is desired to be kept to the encryption server, the encryption server directly communicates with the network of the receiving destination node.

[0052] Therefore, the node on the transmitting side does neither request the encryption server to encrypt data nor transmit the encrypted data to the receiving destination node, so that the exchange of the data with the encryption server can be simplified. That is to say, the time and traffic for one reciprocation required for exchanging the data between the node and the encryption server can be saved, and the processing load on the node on the transmitting side can be reduced, thereby securing the high-speed

performance and efficiency of the data communication.

[0053] The node on the receiving side can receive the encrypted data transmitted from the node on the transmitting side by the encryption server connected to a self network as the restored data. For this reason, the time and traffic for one reciprocation required for exchanging the data between the node and the encryption server can be saved similarly, and the processing load put on the node on the receiving side can be saved, thereby securing the high-speed performance and efficiency of the data communication.

[0054]

[Effect of the Invention] As described above, in the local area network according to the present invention, the encryption and decoding of data are performed not by each terminal device of the network but by the encryption server in a centralized manner. For this reason, the processing load put on each terminal device can be reduced, and it is only necessary to change the settings of the encryption server at the time of changing the encryption key and the encryption method in the network. As a result, a complicated operation for changing the settings of each terminal device does not have to be performed, and thus the network can be easily managed.

[0055] When the communication can be held between the terminal devices in a plurality of networks via an external network, even if data is transmitted/received through any network routes, the data contents are not in danger of being intercepted by outsiders on such routes.

[0056] Further, each terminal device in the networks transmits an encryption key necessary for the encryption or decryption of data to the encryption server, and the encryption server encrypts or decrypts the data based on the encryption key received from each terminal device, so that various encryption methods can be easily utilized.

[Brief Description of the Drawings]

[Fig. 1] Fig. 1 is a diagram illustrating a system structure of a local area network (LAN) according to one embodiment of the present invention.

[Fig. 2] Fig. 2 is a flowchart illustrating a flow of data when encrypted communication is held from a node A to a node C in Fig. 1.

[Fig. 3] Fig. 3 is a flowchart illustrating a flow of data when the encrypted communication is held from the node A to node C by using a routing function of encryption servers S1 and S2 in Fig. 1.

[Fig. 4] Fig. 4 is a diagram illustrating a format of an IP header of a packet transmitted/received between the nodes.

[Fig. 5] Fig. 5 is a diagram illustrating a format of an "Options" field of the IP header.

[Explanations of Letters or Numerals]

A to C: terminal device (node)

S1, S2: encryption server

R1 to R4: Router

NET-1 to NET-3: IP network

NET-4, NET-5: network

FIG. 1

1: ENCRYPTION SERVER

2: NODE

3: ROUTER

FIG. 5

1: OPTION TYPE

2: OPTION LENGTH

3: OPTION DATA

FIG. 2

1: NODE A

2: ENCRYPTION SERVER S1

3: NODE C

4: INITIALIZE

5: REGISTER ADDRESS OF ENCRYPTION SERVER S2 OF LOCAL NETWORK

6: ENCRYPTION SERVER S2

7: INITIALIZE

8: REGISTER ADDRESS OF ENCRYPTION SERVER S1 OF LOCAL NETWORK

9: TRANSMIT ONE PACKET

10: SET ENCRYPTION REQUEST FLAG FOR PACKET HEADER

11: TRANSMIT TO ENCRYPTION SERVER S1

12: RECEIVE

13: ENCRYPT

14: SET ENCRYPTED FLAG

15: TRANSMIT TO NODE A

16: TRANSMIT TO NODE C

17: WHILE PASSING THROUGH EXTERNAL NETWORK, DATA IS BEING ENCRYPTED.

18: TRANSMIT TO ENCRYPTION SERVER S2

19: SET DECRYPTION REQUEST FLAG

20: DECRYPT

21: SET DECRYPTED FLAG

22: TRANSMIT TO NODE C

FIG. 3

1: NODE A

2: ENCRYPTION SERVER S1

3: ENCRYPTION SERVER S2

4: NODE C

5: AT THE TIME OF INITIALIZATION: USE DEFAULT ROUTER AS ENCRYPTION SERVER S1

6: TRANSMIT

7: TRANSMIT TO ENCRYPTION SERVER S1

8: RECEIVE

9: ENCRYPT

10: SUBSTITUTE RECEPTION OF NODE C

11: DATA IN THIS ZONE IS ENCRYPTED.

12: EXTERNAL NETWORK

13: DECRYPT

14: TRANSMIT TO NODE C

15: END

(54) [TITLE OF THE INVENTION] LOCAL AREA NETWORK

(57) [ABSTRACT]

[OBJECT] To enable data to be encrypted and transmitted/received between terminal devices without encrypting and decoding the data between the respective terminal devices.

[CONSTITUTION] An encryption server S1 converts original data transmitted from a node A as a terminal device of a transmitting source of an IP network NET-1 into encrypted data so as to return to the node A, and the node A transmits the encrypted data to a node C as a terminal device of a transmitting source of an IP network NET-3. On the other hand, an encryption server S2 decrypts and restores the encrypted data transmitted from the node C as the terminal device of a receiving destination of the IP network NET-3 into original data so as to return it to the node C.

[CLAIMS]

[Claim 1] A local area network where a plurality of terminal devices are connected by a network so that data can be transmitted/received between the terminal devices, the network comprising an encryption server having a unit for converting original data transmitted from the terminal device of a transmitting source into encrypted data so as to return it to the terminal device as the transmitting source, decrypting the encrypted data transmitted from the terminal device of a receiving destination and restoring it into the original data so as to return the original data to the terminal device of the receiving source.

[Claim 2] A local area network where a plurality of networks is connected so that data can be transmitted/received between a plurality of terminal devices, each of the networks comprising an encryption server having a unit for converting original data transmitted from a terminal device of a transmitting source into encrypted data so as to transmit the encrypted data to a terminal device of a receiving destination of different network, decrypting the encrypted data received from different network and restoring it into the original data so as to transmit the original data to the terminal device of the receiving destination.

[Claim 3] The local area network according to claim 1, wherein

each of the terminal devices has a unit for transmitting an encryption key necessary for encrypting or decrypting data to the encryption server,

the encryption server has a unit for encrypting or decrypting the data based on the encryption key received from each of the terminal devices.

[Detailed Description of the Invention]

[0001]

[Field of Industrial Application] The present invention relates to a local area

network for connecting a plurality of terminal devices via the network.

[0002]

[Prior Art] Conventionally, in a local area network (hereinafter, “ LAN”) complying with standards of Ethernet or IEEE802.3, in order to keep secret of the contents of packets transmitted/received between respective terminal devices (hereinafter, “nodes”), the contents of the packets to be transmitted from on a node on a transmitting side are encrypted by a predetermined encryption system so as to be transmitted to a node of a destination node, and the received and encrypted packets are decrypted and restored into original data contents on the node on receiving side of the destination.

[0003] The encryption system is a technique that converts information understandable by anybody into meaningless code texts based on a predetermined encryption key (simply “key”), and decrypts the code texts using the same encryption key used in the encryption so as to restore them into the original information (referred to as “decoding”).

[0004] In general, a common key encryption system such as a DES encryption method and an FEAL encryption method complying with standard encryption are known as the encryption system. In the common key encryption system, identical encryption key and decoding key are shared between transmitters and receivers, and data are encrypted and decoded (restored) by using the common key.

[0005]

[Problem to be Solved by the Invention] However, since the encryption of packets for keeping communication secrets is not standardized in the above conventional LAN, the contents of the packets should be encrypted at a node on a transmitting side so as to be transmitted, and the encrypted data contents of the received packets should be decrypted so as to be restored into

the original data at a node on a receiving sides.

[0006] Therefore, a processing load is put on the respective nodes, and further when the encryption key and the encryption system (decryption method) are changed, the settings of all the nodes on LAN should be changed. This is very inconvenient.

[0007] Further, in a local network environment, since a network is in a managed state or is easily managed, reliability of the network is high. However, communication is enabled between a plurality of terminal devices in a plurality of networks via an external network, routes of networks through which data are transmitted/received and reach a destination cannot be obtained. For this reason, there arises a problem that the data contents may be intercepted by outsiders on such routes.

[0008] The present invention is devised in view of the above point, and its object is to enable data to be encrypted and transmitted/received between terminal devices without encrypting and decoding in the respective terminal devices.

[0009]

[Means for Solving the Problem] In order to achieve the above object, the present invention provides a local area network where a plurality of terminal devices is connected by a network so that data can be transmitted/received between the terminal devices, the network comprising an encryption server having a unit for converting original data transmitted from the terminal device of a transmitting source into encrypted data so as to return it to the terminal device as the transmitting source, decrypting the encrypted data transmitted from the terminal device of a receiving destination and restoring it into the original data so as to return the original data to the terminal device of the receiving source.

[0010] Further, the invention provides a local area network where a plurality of networks is connected so that data can be transmitted/received between a plurality of terminal devices, each of the networks comprising an encryption server having a unit for converting original data transmitted from a terminal device of a transmitting source into encrypted data so as to transmit the encrypted data to a terminal device of a receiving destination of different network, decrypting the encrypted data received from different network and restoring it into the original data so as to transmit the original data to the terminal device of the receiving destination.

[0011] Further, in the above local area network, each of the terminal devices has a unit for transmitting an encryption key necessary for encrypting or decrypting data to the encryption server, and the encryption server has a unit for encrypting or decrypting the data based on the encryption key received from each of the terminal devices.

[0012]

[Function] In the local area network of the present invention, the encryption server provided to the network converts original data transmitted from the terminal device of the transmitting source into encrypted data and returns it to the terminal device of the transmitting source, decrypts the encrypted data transmitted from the terminal device of the receiving destination so as to restore it into the original data, and returns the original data to the terminal device of the receiving destination. For this reason, the data can be encrypted and transmitted/received between the terminal devices without encrypting and decrypting the data in the respective terminal devices.

[0013] Further, each of the encryption servers provided to a plurality of connected networks convert original data transmitted from the terminal device of the transmitting source into encrypted data so as to transmit it to a

terminal device of the receiving destination in different network, and decrypts the encrypted data received from the different network so as to restore it into the original data, and transmits the original data to the terminal device of the receiving destination. For this reason, the data can be encrypted and transmitted/received between terminal devices in the respective networks without encrypting and decoding the data in the respective terminal devices.

[0014] Further, each of the terminal devices transmits an encryption key necessary for encrypting and decrypting data to the encryption server, the encryption server encrypts or decrypts the data based on the encryption key received from each of the terminal devices. As a result, the encryption and decoding can be performed according to the encryption method based on the encryption key.

[0015]

[Embodiments] Embodiments of the present invention are described concretely below with reference to drawings. Fig. 1 is a diagram illustrating a system structure of a local area network (LAN) according to one embodiment of the present invention. This local area network uses a TCP/IP protocol. This local area network includes three IP networks NET-1, NET-2 and NET-3.

[0016] The IP network NET-1 is connected to terminal devices (nodes) A and B containing a microcomputer composed of CPU, ROM and RAM, and is connected to an encryption server S1 that is one kind of a terminal device having a microcomputer and encrypts and decrypts (restores) data of the nodes A and B, and is connected to a router (referred to as "gateway") R1 for routing a packet between two networks.

[0017] Further, the IP network NET-2 is connected to routers R2 and R3 for routing a packet between two networks. Further, the IP network NET-3 is

connected to a node C containing a microcomputer, and is connected to an encryption server S2 that is one kind of a terminal device containing a microcomputer and encrypts and decrypts (restores) data of the node C. The IP network NET-3 is connected to a router R4 for routing a packet between two networks.

[0018] The routers R1 and R2 are connected by a network NET-4, and the routers R3 and R4 are connected by a network NET-5, so that data can be transmitted/received between the nodes A, B and C of the IP networks NET-1 and NET-3. At this time, the encryption servers S1 and S2 can encrypt the data and can decode the received encrypted data (referred to as "encrypted communication").

[0019] The encryption servers S1 and S2 have a unit for converting original data transmitted from a terminal device of a transmitting source into encrypted data so as to return the encrypted data to the terminal device of the transmitting source, and decrypting the encrypted data transmitted from a terminal device of a receiving destination and restoring it into the original data so as to return the original data to the terminal device of the receiving destination. In this case, the same encryption key and the same encryption algorithm are used for the encryption and the decryption.

[0020] Fig. 2 is a flowchart illustrating a flow of data when encrypted communication is held from the node A of the IP network NET-1 to the node C of the IP network NET-3. The case where an encryption key (key code) of the encryption servers S1 and S2 is fixed is described.

[0021] At first, at the time of initialization, the node A registers an address of the encryption server S1 in the local area network, and the node C registers an address of the encryption server S2 in the local area network.

[0022] When transmission for one packet is requested, the node A sets an

“encryption request flag” for the encryption server S1, so as to transmit raw data. The encryption server S1 encrypts the raw data received from the node A using an encryption key according to a preset encryption method, and sets an “encrypted flag” so as to return the data to the node A.

[0023] The node A adds information representing the encrypted data to the encrypted data received from the encryption server S1, and transmits (transfers) the encrypted data to the node C of the IP network NET-3. The information representing the encrypted data may be stored in a header section of the packet.

[0024] On the other hand, the node C checks the header section of the packet received from the node A, and when the information representing the encrypted data is stored, it determines that the packet is the encrypted data. The node C sets a “decryption request flag” for the encrypted data, and transfers the encrypted data to the encryption server S2. The encryption server S2 decrypts and restores the encrypted data received from the node C using the encryption key, and sets a “decrypted flag” so as to return the restored data to the node C. The node C acquires the restored data from the encryption server S2.

[0025] In such a manner, the encryption servers for encrypting and decrypting data are provided to respective networks, and the encryption servers collectively encrypt and decrypt data transmitted/received to/from the respective terminal devices on the networks. For this reason, each of the respective terminal devices does not have to encrypt and decrypt the data.

[0026] Fig. 4 is a diagram illustrating a format of the IP header of the packet, and Fig. 5 is a diagram illustrating a format of an “Options” field of the IP header. The encryption request flag, the encrypted flag, the decryption request flag and the decrypted flag are defined on an option area of the

"Options" field of the IP header.

[0027] Table 1 is a table illustrating one example of option data, and respective flags are, for example, the encryption request flag "0", the encrypted flag "1", the decryption request flag "3" and the decrypted flag "4".

[0028]

[Table 1]

Class	Number	Length	Function
0	0	1	End of Option List
0	1	1	NOP (No Operation)
0	2	11	Restriction on Security and Process
0	3	Variable	Loose Source Routing
0	9	Variable	String Source Routing
0	7	Variable	Record Route
0	8	4	Stream Identifier
2	4	Variable	Time Stamp
1	1	1	Flag 0: Encryption Request 1: Decryption Request 2: Encrypted 3: Decrypted

[0029] An example where when the encrypted communication is held from the node A of the IP network NET-1 to the node C of the IP network NET-3, an encryption key for encrypting and decrypting data is transmitted to the encryption servers S1 and S2 is described below.

[0030] In this case, the nodes A and C have a function for transmitting the encryption key for encrypting or decrypting data to the encryption servers S1

and S2. The encryption servers S1 and S2 have a function for performing the encryption and decryption methods using a plurality of encryption keys, and they encrypt and decrypt data using the encryption keys transmitted from the nodes A and C.

[0031] At first, the node A holds initialization communication that standardizes an encryption key necessary for exchanging encrypted data with the node C. This initialization communication provides the encryption key of the same encryption method to the nodes A and C.

[0032] When original data is transmitted from the node A to the encryption server S1, the encryption key is attached, and the encryption server S1 encrypts the original data using the encryption key. Further, at the time of decrypting the encrypted data, the node C attaches the encryption key when requesting the encryption server S2 to decrypt the encrypted data, and the encryption server S2 restores the encrypted data using the encryption key. The encryption key is defined in “option data” of the IP header shown in Figs. 4 and 5, for example.

[0033] When transmission request of one packet is generated, the node A sets the "encryption request flag" for the encryption server S1, and transmits raw data together with the encryption key. The encryption server S1 encrypts the raw data received from the node A according the encryption method using the encryption key, sets the "encrypted flag" and returns the data to the node A. The node A transmits (transfers) the encrypted data received from the encryption server S1 to the node C of the IP network NET-3.

[0034] On the other hand, when the node C receives the encrypted data from the node A, it sets the "decryption request flag" and transmits the encrypted data as well as the encryption key to the encryption server S2. The encryption server S2 restores the encrypted data received from the node C

according to the decryption method using the encryption key, and sets the "decrypted flag" so as to return the restored data to the node C. The node C obtains the restored data from the encryption server S2. Therefore, in this LAN, a key code is variable.

[0035] An example, that when the encrypted communication is held from node A of the IP network NET-1 to the node B, the encryption key for encrypting and decrypting data is transmitted to the encryption server S1, is described below.

[0036] When transmission request for one packet is generated, the node A sets the "encryption request flag" for the encryption server S1, and transmits raw data as well as an encryption key. The encryption server S1 encrypts the raw data received from the node A according to the encryption method using the encryption key, and sets the "encrypted flag" so as to return the data to the node A. The node A transmits (transfers) the encrypted data received from the encryption server S1 to the node B.

[0037] On the other hand, when the node B receives the encrypted data from the node A, it sets the "decryption request flag" and transfers the encrypted data as well as the encryption key to the encryption server S1. The encryption server S1 restores the encrypted data received from node B according to the decryption method using the encryption key, and sets the "decrypted flag" so as to return the restored data to the node B. The node B obtains the restored data from the encryption server S1.

[0038] In such a manner, when each terminal device requests the encryption server to encrypt and decrypt data, each of them transmits the encryption key necessary for the encryption and decryption together with the data, and the encryption server encrypts and decrypts the data according to the encryption method using the encryption key. For this reason, each of the terminal

devices can easily utilize the data transmission/reception according to various encryption methods. Further, since each node can freely set an encryption key and can select the encryption method for data, the secrecy of the data communication can be further heightened.

[0039] An example of the encrypted communication when a network routing function is provided to the encryption server is described below. The network structure in this case is the same as that of the local area network shown in Fig. 1, but the functions of the nodes A, B and C and the encryption servers S1 and S2 are slightly different.

[0040] The encryption servers S1 and S2 in this example has a unit for converting original data transmitted from the terminal device of the transmitting source into encrypted data so as to transmit the encrypted data to the terminal device of the receiving destination in different network, and decrypting the encrypted data received from another network so as to restore it into the original data and transmit it to the terminal device of the receiving destination.

[0041] Therefore, a network routing function (router) of a network layer is provided to the encryption servers S1 and S2, and the encryption server S1 functions as a node that is a substitute for the node A at which ARP is implemented.

[0042] In an IP network, a plurality of routers can be provided to one network, and in actual communication, a physical address (MAC address) is obtained from an IP address according to an address resolution protocol (ARP), and a communication destination is specified by the physical address so that communication is held (data link layer). Normally, the physical address that is returned from the communication destination is used, but a different node can return it. This is called as the substitute ARP.

[0043] Each network is provided with an encryption server having a network router function and a substitute response function for receiving a packet instead of a receiving node. A transmitting node of the network on a transmitting side sends only data whose communication secret is desired to be kept to the encryption server, and encryption server converts the data into the encrypted data so as to transmit the data to a network of a receiving destination of this data using the network router function.

[0044] On the other hand, the encryption server of the network on the receiving side receives the packet (encrypted data) transmitted from the network on the transmitting side using the substitute response function for receiving the packet instead of the receiving node, and restores the packet so as to transmit the restored data to the receiving node.

[0045] Fig. 3 is a flow chart illustrating a flow of data when the encrypted communication is held between the node A of the IP network NET-1 to the node C of the IP network NET-3. The case where an encryption key (key code) of the encryption servers S1 and S2 is fixed is described.

[0046] The node A registers an address of the encryption server S1 of the local area network at the time of initialization, and the encryption server S1 is used as a default router for carrying out substitute transmission/reception. Further, the node C registers an address of the encryption server S2 of the local area network at the time of initialization, and the encryption server S2 is used as a default router for carrying out substitute transmission/reception.

[0047] Therefore, the encryption server S1 intercepts the data to be transmitted to the node A as the substitute ARP of the node A, and similarly the encryption server S2 functions as the node for implementing the substitute ARP of the node C to intercept the data to be transmitted to the node C.

[0048] At the time of the data transmission from the node A to the node C, the node A transmits raw data to the encryption server S1. The encryption server S1 encrypts the raw data and sets the "encrypted flag" so as to transmit the encrypted data to the router R1. The encrypted data is transmitted to the routers R1, R2, R3 and R4 in this order, and then to the encryption server S2 substitute for the node C.

[0049] The encryption server S2 receives and decrypts the encrypted data, and finally transmits it to the node C. The node C receives the encrypted data transmitted by the node A from the encryption server S2 as the restored data.

[0050] As to the routing function of the encryption server S1 according to the second embodiment, it is only necessary to transmit all received packets to the router R1. As to the routing function of the encryption server S2, it is only necessary to transmit all received packets to the router R2.

[0051] In such a manner, in the case of the packet communication between a plurality of networks, namely, in the case where data is sent to a receiving destination node of an external network, when the node on the transmitting side specifies the receiving destination node and transmits data whose communication secret is desired to be kept to the encryption server, the encryption server directly communicates with the network of the receiving destination node.

[0052] Therefore, the node on the transmitting side does neither request the encryption server to encrypt data nor transmit the encrypted data to the receiving destination node, so that the exchange of the data with the encryption server can be simplified. That is to say, the time and traffic for one reciprocation required for exchanging the data between the node and the encryption server can be saved, and the processing load on the node on the transmitting side can be reduced, thereby securing the high-speed

performance and efficiency of the data communication.

[0053] The node on the receiving side can receive the encrypted data transmitted from the node on the transmitting side by the encryption server connected to a self network as the restored data. For this reason, the time and traffic for one reciprocation required for exchanging the data between the node and the encryption server can be saved similarly, and the processing load put on the node on the receiving side can be saved, thereby securing the high-speed performance and efficiency of the data communication.

[0054]

[Effect of the Invention] As described above, in the local area network according to the present invention, the encryption and decoding of data are performed not by each terminal device of the network but by the encryption server in a centralized manner. For this reason, the processing load put on each terminal device can be reduced, and it is only necessary to change the settings of the encryption server at the time of changing the encryption key and the encryption method in the network. As a result, a complicated operation for changing the settings of each terminal device does not have to be performed, and thus the network can be easily managed.

[0055] When the communication can be held between the terminal devices in a plurality of networks via an external network, even if data is transmitted/received through any network routes, the data contents are not in danger of being intercepted by outsiders on such routes.

[0056] Further, each terminal device in the networks transmits an encryption key necessary for the encryption or decryption of data to the encryption server, and the encryption server encrypts or decrypts the data based on the encryption key received from each terminal device, so that various encryption methods can be easily utilized.

[Brief Description of the Drawings]

[Fig. 1] Fig. 1 is a diagram illustrating a system structure of a local area network (LAN) according to one embodiment of the present invention.

[Fig. 2] Fig. 2 is a flowchart illustrating a flow of data when encrypted communication is held from a node A to a node C in Fig. 1.

[Fig. 3] Fig. 3 is a flowchart illustrating a flow of data when the encrypted communication is held from the node A to node C by using a routing function of encryption servers S1 and S2 in Fig. 1.

[Fig. 4] Fig. 4 is a diagram illustrating a format of an IP header of a packet transmitted/received between the nodes.

[Fig. 5] Fig. 5 is a diagram illustrating a format of an "Options" field of the IP header.

[Explanations of Letters or Numerals]

A to C: terminal device (node)

S1, S2: encryption server

R1 to R4: Router

NET-1 to NET-3: IP network

NET-4, NET-5: network

FIG. 1

1: ENCRYPTION SERVER

2: NODE

3: ROUTER

FIG. 5

1: OPTION TYPE

2: OPTION LENGTH

3: OPTION DATA

FIG. 2

1: NODE A

2: ENCRYPTION SERVER S1

3: NODE C

4: INITIALIZE

5: REGISTER ADDRESS OF ENCRYPTION SERVER S2 OF LOCAL NETWORK

6: ENCRYPTION SERVER S2

7: INITIALIZE

8: REGISTER ADDRESS OF ENCRYPTION SERVER S1 OF LOCAL NETWORK

9: TRANSMIT ONE PACKET

10: SET ENCRYPTION REQUEST FLAG FOR PACKET HEADER

11: TRANSMIT TO ENCRYPTION SERVER S1

12: RECEIVE

13: ENCRYPT

14: SET ENCRYPTED FLAG

15: TRANSMIT TO NODE A

16: TRANSMIT TO NODE C

17: WHILE PASSING THROUGH EXTERNAL NETWORK, DATA IS BEING ENCRYPTED.

18: TRANSMIT TO ENCRYPTION SERVER S2

19: SET DECRYPTION REQUEST FLAG

20: DECRYPT

21: SET DECRYPTED FLAG

22: TRANSMIT TO NODE C

FIG. 3

1: NODE A

2: ENCRYPTION SERVER S1

3: ENCRYPTION SERVER S2

4: NODE C

5: AT THE TIME OF INITIALIZATION: USE DEFAULT ROUTER AS ENCRYPTION SERVER S1

6: TRANSMIT

7: TRANSMIT TO ENCRYPTION SERVER S1

8: RECEIVE

9: ENCRYPT

10: SUBSTITUTE RECEPTION OF NODE C

11: DATA IN THIS ZONE IS ENCRYPTED.

12: EXTERNAL NETWORK

13: DECRYPT

14: TRANSMIT TO NODE C

15: END